Configuresoft

Security, Compliance and Control for the Virtualized World

TECHNICAL BRIEF

Configuresoft RSCA™ Program

Security and Compliance Assessment Provides Immediate Business Value

Abstract

According to analysts, 80% – 90% of Security exposures are the result of improper configuration of critical systems; servers and workstations. Evolving government mandates and regulations often include significant aspects of IT systems configurations. Security of systems and availability of system resources are tightly coupled. The consequences of improper system configurations, non compliance with best practices and non compliance with government mandates and regulations can be devastating to your business operations and may impart legal consequences.

The ***Rapid Security Configuration Assessment*** program (***RSCA™***) from Configuresoft is a program that enables you to get your arms around the vast amount of information required to set a course for Security and Compliance. This document defines the issues at hand and shows how the Configuresoft **RSCA** program directly addresses these issues. The result is immediate business value.

What is the Problem?

Systems security, compliance with IT security standards and government regulations have rapidly become *The Issues* for Information Technology administrators, managers and executives. One of the largest challenges IT professionals face is the overwhelming task of maintaining consistent, secure, and compliant configurations. The questions for IT Managers are *"Where do we start, how do we assess... and how can we remediate it?"*

Mike Nash, Microsoft Vice President of the Security Group in Redmond, stated at the Microsoft World Wide Partner Conference in 2004 that a single activity of outstanding business value for any client is a Security Assessment. This sentiment has been echoed by Microsoft executives and other industry leaders in increasing currency over the past year.

The issue of IT Security is a problem with major significance for IT operations groups as well as at the CxO level. The consequences of improperly configured systems directly affect the security and availability of system resources. The consequences of non compliance with best practices and government mandates may have legal ramifications. The proliferation of multiple varieties of malware; bugs, viruses, spyware and general network threats, as well as the implementation of government regulations and mandates has increased the visibility of security and compliance issues in IT and operations. It is critical that IT departments adopt a best practices approach that includes strict configuration management disciplines. This includes the utilization of proper tools, training and processes required to monitor and administer an IT shop with a focus on Security and compliance. The advent of government regulations and mandates such as HIPAA, Sarbanes – Oxley, FISMA, GLBA and others require accountability for aspects of IT Security. The focus on security is huge. Questions for businesses working to address these issues are "How to Begin" and "What Tools to Use?"

According to reports from Gartner and PWC, 80 – 90% of Security problems result from improper system configuration. Understanding the absolute configuration state of thousands of servers and workstations in a large enterprise is a daunting task. How can IT personnel manage and control configurations when they cannot be sure of what they have "out there?" How can IT professionals make sure systems configurations are following 'best practices' designs and regulatory compliance if they don't know what they have?

Mike Nash, Microsoft VP Security Group, told 5,000 Microsoft Partners at the 2004 World Wide Partner Conference to "Perform a Security Assessment for your Clients."

Configuresoft recognizes and addresses the complexity of security and compliance. Our flagship product Enterprise Configuration Manager (ECM) addresses these complex issues with scalability required for very large enterprises.

Configuresoft has gone beyond the delivery of exceptional technology with two strategic developments; the ***Center for Policy & Compliance*** **(CP&C)** and the ***Rapid Security Configuration Assessment*** **(RSCA™)** program. The CP&C is a center of expertise that includes Configuresoft staff, certified in security and historically involved in auditing IT organizations and professional speaking engagements. The CP&C works to interpret IT best practices, government mandates and other security guidelines and deliver templates for use in ECM allowing a simple assessment of IT systems according to these various security and compliance issues.

RSCA engagements are offered through Configuresoft's Partner network. RSCA is a delivery vehicle for CP&C content, methodologies and tools to ensure security and compliance. The RSCA program is a quick, efficient and effective process to gain rapid understanding and control over enterprise security and compliance issues. By focusing on the configuration of servers and workstations and comparing this massive set of data against templates that describe best practices and regulatory mandates, RSCA gives you the insight you need to secure your enterprise.

About Enterprise Configuration Manager

Configuresoft's flagship Configuration Management solution, Enterprise Configuration Manager, ECM™, is the comprehensive solution to address Configuration, Change and Compliance issues. ECM collects and stores detailed data from Windows Server and Client systems in a very detailed and extensive Configuration Management Data Base (CMDB). ECM includes hundreds of *"Drop & Deploy"* templates (sets of rules that describe what a desired state for a type of server or user group should be), can then be applied to this data to ensure compliance with desired network states. These templates include compliance templates developed by Configuresoft's Center for Policy & Compliance.

Configuresoft's flagship product, ECM, automates the management of configuration settings for Windows-based servers and clients, and enforces security and IT standards. ECM uses various sets of Configuration templates that are designed to determine the state of compliance with the security policy objectives of the templates. ECM can be used to enforce these security policies without human intervention by automatically resetting configurations to their pre-defined standard when they are inadvertently changed. Within the space of configuration

"Configuresoft's Enterprise Configuration Manager (ECM) is a comprehensive management application that addresses virtually all of the most critical management challenges facing today's IT administrator."

Michael Otey, senior technical director, Windows IT Pro.

management and policy remediation, ECM enables the most detailed monitoring available and automatically mitigates any deltas that were assessed ensuring "Dynamic Compliance Controls" throughout the Microsoft® Windows® environment.

Configuresoft's CP&C leverages expertise into the design of ECM templates that are used to assess compliance with best practices and government mandates such as Microsoft Operations and Security Hardening Guides, Sarbanes – Oxley, FISMA, HIPAA, GLBA and others.

What is the CP&C?

The Center is comprised of a team of security and policy experts, IT auditors and early contributors to the Federal mandates and industry best practices. While Configuresoft's goal includes helping administrators better understand and evaluate the security of their network, the driving factor behind the Center is to help the market gain a better understanding of the tools that can help plan and implement automated strategies that effectively address regulatory and policy compliance issues.

The CP&C develops ECM rules and templates that run against ECM data to determine degrees of compliance. CP&C has developed templates for Microsoft Server Hardening Guides, SOX, FISMA, GLBA and HIPAA. ECM customers use these templates to quickly understand the state of compliance with best practices and government mandates. RSCA customers are able to take advantage of ECM and the CP&C templates in a one time service engagement for security and compliance assessment.

What is the RSCA Program?

The *Rapid Security Configuration Assessment,* RSCA™, is an accelerated process that allows clients to assess their IT systems against industry best practices (ex: ITIL and MOF) as well as government mandates and regulations. The CP&C expertise is applied to the development of ECM *Drop & Deploy* Templates, the assessment criteria for RSCA engagements. RSCA engagements include HIPAA, GLBA, and SOX – as well as framework/methodologies based on SANS, COBIT, COSO and ITIL guidelines.

This assessment, delivered by Configuresoft partners, is often used as the first step in the development of best practices that describe the processes and expertise to manage change, configuration and security

"Organizations often lack the time, objectivity and expertise to accurately assess vulnerabilities to their infrastructure," said Chris Farrow, director of the Configuresoft Center for Policy and Compliance. "The RSCA Program is designed to quickly identify what areas in an organization are vulnerable and determine how to protect them. The Program's prioritized action plan provides a running start for securing an organization's most vulnerable assets."

management in your enterprise; you cannot manage what you don't know. RSCA provides awareness of security and compliance issues you need to develop an intelligent action plan.

Insight gained through an RSCA engagement provides clarity regarding the state of security and compliance conditions throughout your enterprise.

Who is Eligible for RSCA?

The proven RSCA program is available to large enterprise clients that are concerned about the security configurations of their Microsoft Windows environment and subsequent issues regarding compliance to IT or governmental standards and regulations.

With an RSCA assessment, Configuresoft partners work closely with you to quickly and accurately evaluate the configuration quality of production system configurations of servers and workstations in your environments. The assessment reports provide management with critical information regarding security of the environment and how these systems comply with best practices and standards. Additionally, the RSCA review provides a valuable snapshot of the state of an IT environment and suggests methods of improvement.

A Simple and Repeatable Process

The RSCA program has been proven through customer experience. The following are the general steps that make RSCA a successful and repeatable process:

Schedule and Plan RSCA: Configuresoft RSCA Partners will schedule an engagement to be performed on site with minimal intrusion to a production environment. The RSCA team will work with the client to define objectives and logistics of the RSCA engagement in detail.

Data Collection: The RSCA Partner uses ECM to collect configuration data from a selected set of servers. In a matter of hours, the necessary data including operating systems, applications, patch data and other critical configuration data is collected.

Data Analysis: The data is then compared to sets of established compliance templates. Working with the client, the team analyzes the date and builds a set of reports to address the objectives of the RSCA engagement. These reports will be presented to IT and CxO management according to the previously defined schedule.

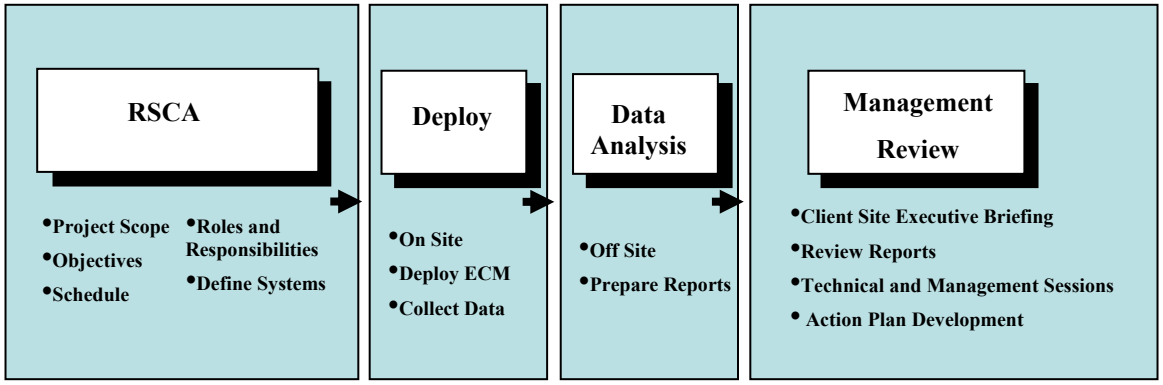
Review and Recommendations: The detailed data is presented to the client by the RSCA team and the client sponsor. The Review meetings usually consist of an Executive summary and Technical IT reports. The

"Within hours of the RSCA engagement, Configuresoft highlighted security patches that were initially thought to be deployed, but instead were not. We immediately went back and fixed all of the items identified."

Bill Randall, director of IT, Red Robin Gourmet Burgers

discussion goes into detail that pertains to the RSCA objectives. Overall status, background issues, areas of improvement, and immediate and

long term remediation methods. Together, the RSCA team and the client develop an action plan to address these findings. The action plan includes a roadmap illustrating a systematic approach for securing and remediation of risk exposures across the enterprise.



The RSCA Program – a vehicle for delivering CP&C methodologies for compliance.

"Organizations often lack the time, objectivity and expertise to accurately assess vulnerabilities to their infrastructure," said Chris Farrow, director of the Configuresoft Center for Policy and Compliance. "The RSCA Program is designed to quickly identify what areas in an organization are vulnerable and determine how to protect them. The Program's prioritized action plan provides a running start for securing an organization's most vulnerable assets."

RSCA Report Output

RSCA assessment reports include operations and security components. Examples of parameters included in these sections are noted in the diagram below. These reports are meant to provide examples of the scope, depth and business value provided by ECM.

Operations Configuration Audit	Security Configuration Audit
Hardware	Local Accounts & Groups
Operating Systems	Service Accounts
IP Settings	Shares
Event Logs	Microsoft Patches

Appendices: Detailed audit findings

Bonus: A complete configuration profile for selected machine

Examples of parameters included in RSCA assessment reports.

RSCA Follow Up Action

Assessments provide valuable information on your IT assets, detailed configuration information and how this data compares with business or government criteria. The longer term business value of RSCA lies in the development and execution of an action plan that addresses any issues of non compliance.

RSCA is often used as a first step to develop best practices that remediate security and audit exposures as well as prevent adverse conditions from recurring. This includes remediation of existing problems, continued checks for on-going compliance, keeping on top of day to day maintenance of those configurations, and tracking changes so you have control and accountability in place? That's where the full functionality of ECM comes into play. By developing a set of skills, processes and tools that define your set of best practices, you can achieve higher levels of availability, improved internal security, more efficient administration, improved performance and service levels, and overall lower costs of ownership.

RSCA - Going Beyond Assessments: Control, Compliance and Change Management

How to Get Started

The RSCA program using Configuresoft's ECM software is available today.

Get Started Today!

www.NetworkingPS.com/RSCA.htm

1-888-717-4010

For information on how to schedule your RSCA engagement, please contact **NetworkingPS** at:

1-888-717-4010 and ask for RSCA,

or visit us on our website at **www.NetworkingPS.com/RSCA.htm**